|| Volume 5 || Issue 12 || April 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH & ENGINEERING TRENDS
Multidisciplinary Journal
Double-Blind Peer Reviewed Refereed Open Access International Journal

A SURVEY ON: NETWORK INTRUSION DETECTION SYSTEM USING MACHINE LEARNING ALGORITHM

Saima Anis Shaikh[1],Sajiya Ayyas Shaikh[2],Purva Jayprakash Sawant[3],Purva Jayprakash Sawant[4],
Shravni Suresh Bale[5], Prof. Tambe.R[6]

Department Of Computer Engineering, Shri. Chhatrapati Shivaji Maharaj College Of Engineering, Ahmednagar, Savirtibai Phule Pune University, India [1,2,3,4,5,6]

123saimas@gmail.com,sajiyashaikh598@gmail.com,purvasawant60@gmail.com,shravnibale2000@gmail.com, ravindra.tambe@scoea.org

----------***----------

Abstract: Network Discovery Mechanism (NIDS) for System Network Interference allows the system manager to detect network security failures. Nevertheless, when designing a smart and efficient NIDS for sudden and capricious assaults, certain problems arise.The study proposed presents a new profound learning paradigm to enable the operation of NIDS in modern networks. The model demonstrates a deep learning mix that is able to analyses a broad spectrum of network traffic correctly. In addition, it offers a new, built-in deep learning classification show with features. The performance assessed data collection, especially the KDD CUP data packet, for network intrusion detection.

Keywords—*Machine learning, intrusion detection, KDD, Network security.*

----------***----------

I INTRODUCTION

A stable and efficient network intrusion detection system is a big challenge in network security (NIDS). Despite significant developments in NIDS, most solutions do use less effective signature-based approaches than anomaly detection strategies. The current problems include the inefficient and unreliable discovery of threats by the latest techniques. Three key drawbacks are needed to enhance the efficiency and precision of network data volumes, in-depth control, as well as the numbers of various protocols and the diversity of data transmission. Mechanical learning and low-level learning approaches were the key subject of NIDS studies. In the initial profound study, its superior layer-specific learning can better or at least be consistent with the success of profound learning techniques. It will make the network data more deeply evaluated and the detection of deviations quicker. In this article, a new profound learning version is proposed which allows NIDS to operate on modern networks.

While the security of the network is increasingly being growing, the current technologies are still unable to completely secure inter-net apps and computer networks from threats from ever increasing cyber-attack methods, such as DoS attacks and computer malware. Therefore, it has become more important than ever to develop successful and flexible safety methods. The standard security strategies, such as user authentication, firewall and data encryption, are inadequate to completely protect the network's hole scene, when facing constantly changing intrusion capabilities and methods[1]. Hence, other line of security defense is more recommended, like Intrusion Detection System (IDS). Currently, an IDS alongside with anti-virus software has become an important complement to the security infrastructure of most organizations. The combination of these two lines provides a more comprehensive defense against those threats and enhances network security. A significant amount of research has been conducted to develop intelligent intrusion detection techniques, which help achieve better network security. Bagged boosting-based on C5 decision trees [2] and Kernel Miner [3] are two of the earliest attempts to build intrusion detection schemes. Methods proposed in [4] and [5] have successfully applied machine learning techniques to classify network traffic patterns that do not match normal network traffic. Both systems were equipped with five distinct classifiers to detect normal traffic and four different types of attacks (i.e., DoS, probing, U2R and R2L).

The IDSs are nevertheless challenged with the latest networking info, which is usually enormous in size[9]. Because of the computational difficulty of managing the data, these large data delay the identification procedure and may contribute to in satisfactory classification precision. The classification of an enormous volume of data generates many mathematical problems, which thus increases the numerical complexity. A typical example of larger intrusion datasets as a popular intrusion estimate dataset is the KDD Cup 99. This dataset includes over five million teaching samples and two million research samples. Such a large-scale dataset checks a classifier's construction and test process or forms an incapable classifier because of frame errors due to low memory. In addition, large-scale datasets typically contain noisy, redundant or informative elements that present crucial challenges in discovering and modelling information.

II.LITERATURE SURVEY

Dong and X. Wang et al. [1] focuses on deep learning methods which are inspired by the structure depth of human brain learn from lower-level characteristic to higher levels concept.

R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao

et al. [2] paper is to review and summarize the work of deep learning on machine health monitoring. The applications of deep learning in machine health monitoring system.

H. Lee, Y. Kim, and C. O. Kim et al. [3] can identify global and invariant features in the sensor signals for fault monitoring and is robust against measurement noise. An SdA is consisting of denoising autoencoders that are stacked layer by layer.

L. You, Y. Li, Y. Wang, J. Zhang, and Y. Yang et al. [4] the feature of short messages is extracted by word2vec which captures word order information, and each sentence is mapped to a feature vector. In particular, words with similar meaning are mapped to a similar position in the vector space, and then classified by RNNs.

R. Polishetty, M. Roopaei, and P. Rad et al. [5] cloud platform is proposed for plate localization, character detection and segmentation. Extracting significant features makes the LPRS to adequately recognize.

K. Alrawashdeh and C. Purdy et al. [6] a deep learning approach for anomaly detection using a Restricted Boltzmann Machine (RBM) and a deep belief network are implemented.

A. Javaid, Q. Niyaz, W. Sun, and M. Alam et al. [7] proposes a deep learning based approach for developing an efficient and flexible NIDS.

S. Potluri and C. Diedrich et al.[8] in this paper choose multi-core CPU's as well as GPU's to evaluate the performance of the DNN based IDS to handle huge network data.

C. Garcia Cordero, S. Hauke, M et al. [9] it proposes a mechanism for detecting large scale network-wide attacks using Replicator Neural Networks (RNNs) for creating anomaly detection models.

T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M.Ghogho et al.[10] apply a deep learning approach for flow-based anomaly detection in an SDN environment.

III.RELATED WORK

The performance of the proposed model is evaluated by the KDD Cup dataset. In order to train classifiers like SVM and ELM, 10 percent KDD training dataset is taken which contains large number of instances. 10 percent KDD dataset is taken rather than entire dataset, because applying entire dataset will cause several problems. Symbolic attributes like protocol, service and flag get changed or removed. Finally, the instances get labeled under four categories: Normal, DoS, Probe, and R2L. They have trained SVM and ELM with the Dataset. For testing process, they have used multi-level model with corrected KDD dataset. Accuracy of the proposed model has attain up to 95.75 percentages and false alarm rate of 1.87 percentages by using KDD Cup 1999 dataset.[11]

Intrusion Detection System (IDS) is a system that identifies, in real time, attacks and takes corrective action to prevent those attacks.

One of the major challenges in network security is the provision of a robust and effective Host - Based Intrusion Detection System (HIDS).

The current issues:

- Volume of data
- Granularity required to improve effectiveness and accuracy

The main focus of HIDS research has been the application of machine learning and shallow learning techniques. By which superior layer-wise features can be learned.

It able to facilitate improved classification results when compared with leading methods such as Deep Belief Networks (DBNs). By combining both machine and shallow learning techniques to exploit their respective strengths and reduce analytical overheads. It can able to be better or at least match results from similar research, whilst significantly reducing the training time.

IV.PROPOSED WORK

Propose a novel deep learning model to enable HIDS operation within modern networks. The model proposes is a combination of deep and machine learning, capable of correctly analyzing a wide-range of network traffic.

More specifically, combine the power of stacking our proposed Non-symmetric Deep Auto-Encoder (NDAE) (deep learning) and the accuracy and speed of Decision Tree (machine learning). KDD Cup '99 and NSL-KDD datasets has used. It is capable of facilitating a deeper analysis of network data and faster identification of any anomalies.

The false positive rate should minimum. (Number of negative events wrongly categorized as positive)To detect intrusion so that system can be prevented from their attacks.

Dataset contains symbolic features; these features are unable to process by the classifier. Hence, pre-processing takes place. In this phase all non-numeric or symbolic features get removed or exchanged. Elimination or replacement of non-numeric or symbolic features is done in pre-processing phase. The overall process of pre-processing is essential, in which non-numeric or symbolic features are eliminated or replaced, as they do not perform any important participation in intrusion detection. Symbolic attributes like protocol, service and flag get changed

or removed. Finally, the instances get labeled under four categories: Normal, DoS, Probe, and R2.[11].

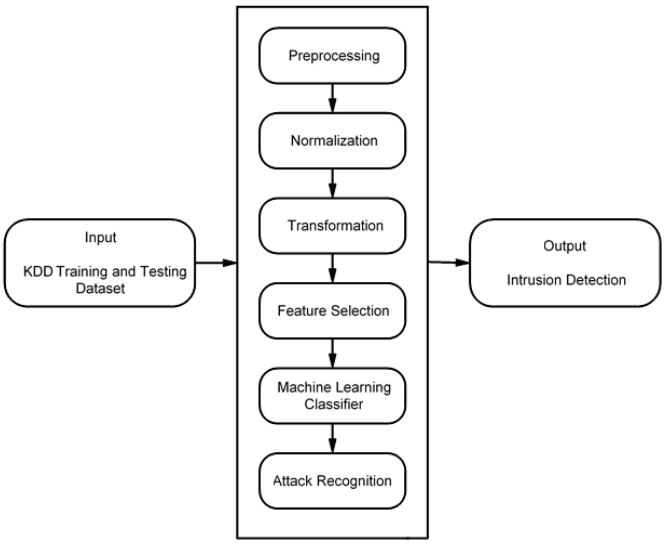

Fig. 1. Overview of the proposed work

V.CONCLUSION

Intrusion detection and Intrusion prevention are needed in current trends. Among them machine learning plays a vital role. HIDS's Framework are used to get high accuracy NDAE approach for unattended functional learning. In this context, we have created a new classification model based on stacked NDAEs and the RF classification algorithm. The intrusion detection framework has already been introduced. This results in a highly accurate, precise and reminiscent technique with decreased preparation time.

REFERENCES

[1]B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in Proc. 8th IEEE Int.Conf. Commun. Softw. Netw, Beijing, China, Jun. 2016, pp. 581–585.

[2]R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, "Deep learning and its applications to machine health monitoring: A survey," Submitted to IEEE Trans. Neural Netw. Learn. Syst., 2016. [Online]. Available: http://arxiv.org/abs/1612.07640

[3]H. Lee, Y. Kim, and C. O. Kim, "A deep learning model for robust wafer fault monitoring with sensor measurement noise," IEEE Trans. Semicond. Manuf., vol. 30, no. 1, pp. 23–31, Feb. 2017.

[4]L. You, Y. Li, Y. Wang, J. Zhang, and Y. Yang, "A deep learning based RNNs model for automatic security audit of short messages," in Proc. 16th Int. Symp. Commun. Inf. Technol., Qingdao, China, Sep. 2016, pp. 225–229.

[5]R. Polishetty, M. Roopaei, and P. Rad, "A next-generation secure cloud based deep learning license plate recognition for smart cities," in Proc. 15th IEEE Int. Conf.Mach. Learn. Appl., Anaheim, CA, USA, Dec. 2016, pp. 286–293.

[6]K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in Proc. 15th IEEE Int. Conf. Mach. Learn. Appl., Anaheim, CA, USA, Dec. 2016, pp. 195–200.

[7]A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proc. 9th EAI Int.Conf. Bio-Inspired Inf. Commun. Technol., 2016, pp. 21–26. [Online]. Available: http://dx.doi.org/10.4108/eai.3-12-2015.2262516

[8]S. Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced intrusion detection system," in Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom., Berlin, Germany, Sep. 2016, pp. 1–8.

[9]C. Garcia Cordero, S. Hauke, M. Muhlhauser, and M. Fischer, "Analyzing flow-based anomaly intrusion detection using replicator neural networks," in Proc. 14th Annu. Conf. Privacy, Security. Trust, Auckland, New Zeland, Dec. 2016, pp. 317–324.

[10]T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Proc. Int. Conf. Wireless Netw. Mobile Commun., Oct. 2016, pp. 258–263.

[11] Anish Halimaa A, Dr. K.Sundarakantham, "MACHINE LEARNING BASED INTRUSION DETECTION SYSTEM" Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8